Revision History

| Version | Date |
|---|---|
| Data Protection Risk Management Policy, 1.0 | 30 July 2021 |

# DATA PROTECTION RISK MANAGEMENT POLICY

## I. Introduction

As provided in the USEIC Data Protection Charter (the "Charter"), the Organization is charged with protecting the confidentiality, integrity, and availability of its Information Resources. To accomplish this task, a formal Data Protection Risk Management Program has been established as a component of the Organization's Data Protection Program to ensure that the Organization is operating with an acceptable level of risk. The Data Protection Risk Management Program is described in this Policy.

Capitalized terms used in this Policy without definition are defined in the Charter.

## II. Policy

Information Security Risk Management covers all of the Organization's Information Resources, whether managed or hosted internally or externally. Executive Managers, System Owners, Data Owners, and IT Custodians are responsible for working with the Data Protection Officer (DPO) to implement the Data Protection Risk Management Program, including remediation of identified risks in a timely manner.

The Data Protection Risk Management Program is comprised of the following processes:

### A. Information Resources Risk Categorization

All Information Resources that store, process, or transmit Organizational Data are included in the Data Protection Risk Management Program. Information Resources are categorized based on their function, threat exposure, vulnerabilities, and Organizational Data type pursuant to the Data Protection Policies. The categorization process takes into account the following elements:

- Size, complexity and capabilities of the Information Resources and organizations;
- Technical infrastructure, hardware, and software capabilities;
- Cost of implementing security controls; and
- Probability and criticality of risks to Organizational Data, particularly Sensitive Data or Confidential Data.

Resources to address risks are allocated according to the identified risks.

### B. Security Control Selection

The appropriate security controls to mitigate identified risks are selected based on the nature, feasibility, and cost effectiveness of the controls. The Organization has selected elements from the following security control frameworks to use as part of its Data Protection Risk Management Program:

- ISO 27002, Security Techniques – Code of Practice for Information Security Management;
- ITIL- Industry Standard Framework for IT Service Management Guidelines and Best Practices;

All Systems and Endpoints must meet the baseline requirements as defined in the USEIC Registration and Protection of Systems Policy or the USEIC Registration and Protection of Endpoints Policy. Additional controls will be evaluated based on the framework defined above and applied based on risk analysis.

## C. Risk Analysis

A documented risk analysis process is used as the basis for the identification, definition, and prioritization of risks. The risk analysis process includes the following:

- Identification and prioritization of the threats to Information Resources;
- Identification and prioritization of the vulnerabilities of Information Resources;
- Identification of a threat that may exploit a vulnerability;
- Qualitative identification of the impact to the confidentiality, integrity, and availability of Information Resources if a threat exploits a specific vulnerability; and
- Identification and definition of measures and/or controls used to protect the confidentiality, integrity, and availability of Information Resources.

The risk analysis process is updated when environmental, operational, or technical changes arise that impact the confidentiality, integrity, or availability of Information Resources. Such changes include:

- New threats or risks with respect to the Information Resources;
- An information security incident;
- Changes to information security requirements or responsibilities. (e.g., new national or international law or regulation, new role defined in the Organization, new or modified security controls implemented, etc.); and
- Changes to USEIC's organizational or technical infrastructure that impact Information Resources (e.g., addition of a new network, new hardware/software standard implemented, new method of creating, receiving, maintaining, or transmitting Data, etc.).

When security measures for an Information Resource do not meet a security standard, risks are identified and expressed. Three factors are considered when determining the risk:

- The type of possible threat and its likelihood;
- The extent of effectiveness of current security controls or their vulnerability; and
- The likely level of impact.

Risks are qualitatively expressed as Critical, High, Medium, Low and Minimal. For purposes of this Policy, Critical, High, Medium, Low and Minimal Risks are defined as follows:

- Critical Risk: The risk of imminent compromise or loss of Sensitive Data from either external or internal sources or where Sensitive Data has already been exposed. There is no control in place to protect such Data.
- High Risk: The risk of imminent compromise or loss of Sensitive Data from either external or internal sources. There is only a single control, or multiple ineffective controls, in place to protect such Data.
- Medium Risk: The risk of compromise or loss of Sensitive Data is possible from either external or internal sources, although less likely from external sources. Controls are in place that are somewhat effective to protect such Data.
- Low Risk: The risk of compromise or loss of Sensitive Data is possible, but not probable or an Information Resource might be used to obtain access to Sensitive Data on a different Information Resource.
- Minimal Risk: There is no realistic risk of compromise or loss of Sensitive Data.

## D. Risk Remediation

The strategies for risk remediation are proportionate to the risks to the Information Resource. The selected and implemented risk management measures reasonably protect the confidentiality, integrity and availability of Information Resources and the risk is managed on a continuous basis. One or more of the following methods are used to manage risk:

- Risk elimination, mitigation, or reduction;
- Risk avoidance;
- Risk acceptance; and/or
- Risk transference.

A Low or Minimal Risk may be accepted by an Executive Manager with appropriate documentation and periodic review. If a previously accepted risk is realized in a real incident, the risk analysis and management are repeated with the new information and re-addressed with greater sensitivity and urgency based on the nature and extent of the incident.

## E. Risk Monitoring

The results of Risk Analysis and Risk Remediation are documented and reviewed by Executive Managers, the DPO, System Owners, Data Owners, and IT Custodians. Monitoring processes are used to evaluate:

- The effectiveness of security controls;
- Changes to Information Resources and environments of operations; and
- Compliance with national and international laws and regulations, industry standards and organizational policies.

The frequency of risk monitoring will be based on:

- Regulatory compliance requirements;
- The importance or sensitivity of the Information Resource;
- The requirements of the Data Protection Policies; and
- The degree to which Systems are interconnected to one another and the risk posed by such connections.